



US010262138B2

(12) **United States Patent**
Boutnaru

(10) **Patent No.:** **US 10,262,138 B2**
(45) **Date of Patent:** **Apr. 16, 2019**

(54) **TECHNIQUES FOR RANSOMWARE
DETECTION AND MITIGATION**

(71) Applicant: **PAYPAL, INC.**, San Jose, CA (US)

(72) Inventor: **Shlomi Boutnaru**, Moddin (IL)

(73) Assignee: **PAYPAL, INC.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 197 days.

(21) Appl. No.: **15/266,974**

(22) Filed: **Sep. 15, 2016**

(65) **Prior Publication Data**

US 2018/0075239 A1 Mar. 15, 2018

(51) **Int. Cl.**
G06F 21/56 (2013.01)
G06F 21/60 (2013.01)
G06F 21/55 (2013.01)

(52) **U.S. Cl.**
CPC **G06F 21/566** (2013.01); **G06F 21/554**
(2013.01); **G06F 21/60** (2013.01); **G06F**
2221/034 (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,797,022 A * 8/1998 Shimotono G06F 1/32
711/135
9,436,824 B1 * 9/2016 Levchenko G06F 9/46

9,514,309 B1 * 12/2016 Mann G06F 21/56
2013/0111547 A1 * 5/2013 Kraemer G06F 21/552
726/1
2017/0364681 A1 * 12/2017 Roguine G06F 21/554
2018/0018458 A1 * 1/2018 Schumugar G06F 21/566

OTHER PUBLICATIONS

Friedman, Mark, et al. "File Cache Performance and Tuning"
[Online] Windows 2000 Performance Guide [retrieved on Aug. 15,
2016]. Retrieved from the Internet: <URL: [https://msdn.microsoft.com/enus/library/bb742613\(d=printer\).aspx](https://msdn.microsoft.com/enus/library/bb742613(d=printer).aspx)>, Jan. 2002.
Evans, Chris "Write-through, write-around, write-back: Cache explained"
[Online] [retrieved on Aug. 15, 2016]. Retrieved from the Internet:
<URL: <http://www.computerweekly.com/feature/WritethroughwritearoundwritebackCacheexplained>>.

(Continued)

Primary Examiner — Alexander Lagor

(74) Attorney, Agent, or Firm — Haynes and Boone, LLP

(57) **ABSTRACT**

An attacker who gains control of a computer system using malicious software (malware) may be able to do anything to the data on the system. One type of malware, sometimes referred to as ransomware, can encrypt the contents of a hard drive or other data repository, preventing those contents from being accessed by their rightful owners. A ransomware attack can be greatly disruptive to an individual or business, and result in loss of data and loss of computer system uptime, impacting overall computing productivity. By detecting that ransomware is operating on a computer (e.g. by correlating between the original data and content in different cache layers), the negative effects of the ransomware may be mitigated or avoided.

20 Claims, 7 Drawing Sheets

